Secure data exchange for electronic or internet payments

Patent number:	FR2788154
Publication date:	2000-07-07
Inventor:	BARON DENIS PHILIPPE
Applicant:	PHILIPPE BARON D (FR)
Classification:	
- International:	G07F7/10; H04L9/32; G06K19/07; G06F1/00
- european:	G07F7/10D4
Application number:	FR19980015439 19981201
Priority number(s):	FR19980015439 19981201

Abstract of **FR2788154**

The security technique is based on storage of a large number of personal codes on the system, and using a different code for each transaction. Thus an intercepted code cannot be reused successfully. This can be used in conjunction with techniques such as matching a clock signal, authentication of a storage device or identification of the person operating the system.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 788 154**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 15439**

(51) Int Cl[7] : G 07 F 7/10, H 04 L 9/32, G 06 K 19/07, G 06 F 1/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 01.12.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 07.07.00 Bulletin 00/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *BARON DENIS PHILIPPE* — FR.

(72) **Inventeur(s) :** BARON DENIS PHILIPPE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) SUPPORTS ET SYSTEMES D'ECHANGE DE DONNEES SECURISES NOTAMMENT POUR PAIEMENTS ET TELEPAIEMENTS.

(57) Supports et systèmes d'échange de données sécurisés notamment pour paiements et télépaiements.

L'échange de données informatiques confidentielles, le paiement par carte bancaire, sur place ou à distance par l'intermédiaire d'un réseau pose le problème de la sécurisation: indiquer son code personnel c'est risquer de le voir réutilisé délictueusement.

Le principe de base de l'invention consiste à stocker un grand nombre de codes sur le support servant à un échange d'informations ou à un paiement et à utiliser un code différent pour chaque opération réalisée. Ainsi si un code est intercepté, il ne peut être réutilisé.

D'autres moyens peuvent être mis en oeuvre comme l'association des données à un signal comme un signal d'horloge, l'authentification du support, l'identification du possesseur du support.

L'invention vise à proposer de nouveaux supports (cartes de paiement, disques à lecture optique et/ ou magnétique...) et de nouveaux systèmes d'exploitation sécurisés sans utiliser nécessairement de nouveaux lecteurs de supports.

FR 2 788 154 - A1

La présente invention se situe dans le domaine de la reconnaissance des intervenants et de la sécurisation des échanges de données informatiques principalement entre ordinateurs qui se transmettent des données numériques en clair, codées ou cryptées notamment en vue d'un paiement électronique ou d'un télépaiement.

Quel que soit le niveau de complexité ou de sophistication d'un système de sécurisation de télépaiement ou de paiement sur place utilisant une certification comportant un échange de données même cryptées ou créant ou reconnaissant une signature numérique, la communication, le transfert de données peuvent toujours être piratés pour être utilisés délictueusement avec des matériels de plus en plus sophistiqués et des pirates de plus en plus ingénieux lorsqu'il s'agit de données, de codes ou de signatures numériques pouvant être réutilisés. Le piratage peut s'en prendre aux ordinateurs eux-mêmes par exemple avec l'intrusion de virus du type "cheval de Troie" qui permettent, entre autres, de reconnaître et stocker un code secret lorsqu'il est utilisé dans l'ordinateur pour ensuite en expédier délictueusement une copie vers un autre ordinateur; ce piratage peut s'en prendre aussi aux communications entre les ordinateurs (ou les périphériques tels que lecteurs de cartes à puces) quelles que soient les voies utilisées (lignes téléphoniques électriques, fibres optiques, liaisons satellites ou autres).
La réutilisation délictueuse de données piratées à l'insu des utilisateurs légitimes de ces données est le point faible de la sécurisation des échanges de données numériques et particulièrement de tout moyen de paiement électronique ou de télépaiement.

Afin de remédier à ces inconvénients et selon une première caractéristique, le dispositif selon l'invention comporte un support qui utilise des données en vue de la sécurisation ne pouvant être exploitées qu'une seule fois. Ces données sont de préférence stockées sous la forme d'un grand nombre de codes et/ou d'algorithmes sur ledit support utilisé pour l'échange (par exemple un paiement), de préférence disposés dans une seule liste et ne pouvant être exploités un par un qu'une seule fois. De préférence dans le système informatique du destinataire, un deuxième stockage de données identiques à celles stockées sur ledit support et dans le même ordre permet d'identifier chaque code proposé comme provenant bien dudit support. Chaque fois qu'un code est échangé entre deux dispositifs informatiques, il est rendu inutilisable, c'est le code suivant dans

la liste des codes qui sera utilisable pour l'échange suivant. Ainsi de telles données interceptées délictueusement ne peuvent être réutlisées par un pirate.

Dans toute la présente description ainsi que dans les revendications, les termes suivants sont utilisés selon la définition indiquée pour la compréhension mais non restrictive:

- autorité: organisation qui émet et/ou gère l'utilisation des supports en vue de l'acceptation ou du refus d'une authentification, d'un paiement, d'un télépaiement,
- banque: c'est dans certains cas l'autorité; elle peut déléguer tout ou partie de ses pouvoirs à une tierce partie qui devient l'autorité dans le système de sécurisation des échanges,
- commerçant: fournisseur de produits et/ou de services,
- code: il peut s'agir d'au moins un mot, au sens informatique, et/ou d'au moins un algorithme,
- échange: envoi de données numériques d'un émetteur vers un récepteur; la communication de données peut se faire dans les deux sens pendant le même échange et permet l'envoi de messages, codes,...afin de réaliser une opération complète comme un paiement avec vérifications sur les intervenants; l'échange peut s'effectuer sur place par le porteur par exemple par un paiement par carte à puce, ou à distance par exemple par l'intermédiaire d'un ordinateur relié à un autre ordinateur par une ligne téléphonique,
- numérique: est employé dans le sens du système qui est employé par les ordinateurs, en principe le système binaire, et qui peut être représenté par d'autres systèmes (octal, hexadécimal,...) ou complété par un système à valeurs intermédiaires issu de la logique floue,
- pirate: un individu ou un groupe qui commet des actes délictueux afin de tenter de détourner, de s'approprier des informations confidentielles pour elles-mêmes ou pour se substituer à un commerçant, à un porteur ou à une autorité pour détourner des fonds à son profit; il peut agir à tous les niveaux d'un échange: vol d'un support, intrusion dans les échanges informatiques pour produire de faux supports ou de fausses données informatiques...,
- porteur: c'est le possesseur authentique d'un support avec lequel il peut effectuer des échanges avec un commerçant, avec sa banque ou avec une autre entité, sur place ou à distance,
- support: dispositif où l'on peut inscrire en mémoire des données informatiques et comportant également des fonctions permettant, entre autres, d'effectuer des échanges; le support peut être une carte, de préférence de type carte bancaire,

ou un disque (disquette, CD ROM ou autre) à lecture magnétique et/ou optique ou un objet quelconque (bague, montre, monture de lunettes, porte-clés, pendentif, ...) pouvant intégrer un système informatique nécessaire à un échange sécurisé par l'intermédiaire d'un dispositif informatique tel qu'un ordinateur avec ou sans l'aide d'un lecteur. Le support peut aussi être autonome, à l'exception éventuellement d'une source d'énergie, et se passer de l'intermédiaire d'un ordinateur pour effectuer des échanges avec des matériels informatiques.

Selon des modes particuliers de réalisation:

- la(les) liste(s) de codes peut(peuvent) être complétée(s) ou remplacée(s) par au moins un algorithme capable de créer des codes au fur et à mesure de la nécessité résultant de l'utilisation du support; au moins un algorithme installé dans le système informatique de l'autorité crée les mêmes codes pour les comparer à ceux du support quand un échange avec ce support nécessite une authentification dudit support.
- les données concernant un échange, une opération quelconque en clair, codées ou cryptées peuvent être associées à au moins un code de la liste inscrite sur le support ou créée par le système de ce dernier.
- le support n'est utilisable que par l'intermédiaire d'un petit nombre d'ordinateurs particuliers (de préférence un seul ordinateur) pour réaliser des échanges.
- l'utilisation du support peut être soumise à un code variable propre au possesseur du support.
- un code piégé peut interdire l'utilisation du support en cas de tentative d'utilisation de ce code.
- un dispositif de détection utilisant par exemple au moins un signal d'horloge ou tout autre signal ayant la même fonction peut être associé au système pour s'assurer que chaque échange est transmis en totalité, en temps réel et sans interruption.
- les caractéristiques d'au moins un signal d'horloge ou de tout autre signal ayant la même fonction peuvent présenter des variations prévues, de préférence secrètes.
- le support peut ne fonctionner, lorsqu'il est sollicité pour un échange, que si l'autorité lui adresse au moins un code, qui change de préférence à chaque échange ou tentative d'échange que ledit support reconnait, après quoi seulement il produit des données d'identification que l'autorité devra reconnaître.
- l'identification du porteur peut se faire par plusieurs moyens dont un dispositif secondaire indispensable au fonctionnement du support.

Dans une forme de réalisation nullement limitative, le dispositif objet de l'invention se présente sous la forme d'un support pouvant, notamment, stocker une grande quantité de données numériques de préférence sous forme de codes qui sont disposés dans au moins une liste rendue inaccessible à la consultation ou à la modification une fois qu'elle est inscrite dans la mémoire du support, sauf pour le premier code de cette liste qui peut être consulté, utilisé par exemple pour une authentification dans un échange. De par la conception du support, chaque code ne peut être utilisé qu'une seule fois après quoi il peut être écarté, effacé ou rendu inaccessible et c'est le code suivant de ladite liste qui est alors le seul code consultable, utilisable et chaque fois sous certaines conditions décrites ci-après.

Lesdits codes contenus dans au moins une liste se succèdent de manière imprévisible, pour un observateur extérieur à la mise en place de la liste et à sa confidentialité, sont conçus par exemple de manière aléatoire grâce à un logiciel dont dispose l'autorité qui réalise et qui dispose des codes dans deux listes absolument identiques, l'une est inscrite sur un support qui sera fourni à un porteur autorisé, connu de l'autorité, l'autre reste en mémoire dans le système informatique de l'autorité. Une telle disposition aléatoire d'un grand nombre de codes permet de réaliser avec le même logiciel un grand nombre de listes différentes les unes des autres attribuables à un grand nombre de porteurs.

Ledit support permet d'échanger des données informatiques servant à l'autorité à authentifier le support pour ensuite échanger des données qui peuvent être confidentielles, qui engagent les intervenants qui peuvent être par exemple propres à une entreprise qui correspond avec ses succursales ou tout autre type d'échange de données que l'on veut garder confidentielles ce qui permet notamment de sécuriser un paiement sur place, sur le lieu de la transaction grâce au support utilisé dans ce but ou de sécuriser un télépaiement réalisé par exemple grâce à un ordinateur relié à un réseau informatique.

Dans le cas où les données sont confidentielles, un codage ou un cryptage sont de préférence utilisés avec un degré plus ou moins élevé du niveau de confidentialité tout en respectant la règlementation du(des) Etat(s) où ces données doivent circuler.

De préférence et contrairement au mode de fonctionnement du support, le système informatique de l'autorité peut consulter les codes précédents et les codes suivants dans sa propre mémoire lors d'un échange afin d'éviter un blocage de ce type d'échange si, à la suite d'une mauvaise manipulation du porteur ou une mauvaise transmission des données, un code doit être éliminé

pour laisser place au suivant alors que l'autorité n'a pas encore enregistré ce dernier code émis par le support.

Pour éviter une substitution du support émis ou validé par l'autorité par un faux support ayant apparemment le contenu d'un support authentique, en essayant de trouver le bon code en en réalisant un grand nombre et en les proposant un par un à l'autorité, au bout d'un certain nombre de tentatives qui ne fournissent pas le bon code, nombre prédéterminé en accord avec le porteur authentique, le système informatique de l'autorité peut bloquer l'utilisation de ce support, en informer par exemple le commerçant auprès duquel un paiement est en cours ou conserver le support si la tentative se fait auprès d'un distributeur de billets par exemple. Après un blocage de ce type, le support peut être définitivement inutilisable ou bien le porteur devra fournir la preuve de son identité en se rendant physiquement auprès de l'autorité pour constater qu'il est bien le porteur autorisé et débloquer l'utilisation de ce support dans le système informatique de l'autorité. Cette contrainte est en réalité une mesure de sécurité contre l'utilisation d'un faux support au nom d'un porteur autorisé et à son insu. Pour le porteur autorisé ce type de blocage ne devrait jamais être appliqué dans un usage normal du support.

Par cette caractéristique des listes identiques sur le support et dans le système informatique de l'autorité, celle-ci élimine les risques:

- d'utilisation et de paiement avec un faux support,
- d'un télépaiement délictueux en ayant piraté les données numériques échangées, lors d'un paiement ou d'un télépaiement précédent, entre un support et une autorité.

Quel que soit le degré de technologie mis en oeuvre pour un tel piratage, le code utilisé pour un paiement ou un télépaiement avec un support sécurisé comme décrit plus haut étant utilisé et donc consultable seulement pour un seul échange et n'étant plus valable pour un autre échange, les données piratées sont inexploitables.

Cependant un piratage évolué, lors d'un paiement, pourrait consister à détourner la voie de communication entre le commerçant et la banque. A la prise de contact du commerçant avec la banque du porteur, la communication parviendrait en fait à une fausse banque qui pourrait interroger le support présenté, en extraire le premier code, renvoyer au commerçant de fausses données d'acceptation du paiement pour ne pas donner l'éveil même si ce paiement n'a pas lieu et utiliser immédiatement le code fourni par le support pour une autre transaction au détriment du porteur du commerçant ou de la banque

selon les accords préalables entre les participants.
Bien que ce type d'agissement demande une haute technicité, il est bon de s'en prémunir par exemple en dotant le commerçant d'un système semblable à celui décrit plus haut comportant au moins un couple de deux listes identiques de codes dont on ne peut consulter qu'un code à la fois mais dans cette utilisation des listes de codes c'est le commerçant qui est l'autorité afin de reconnaître, d'authentifier la banque du porteur. Les banques désirant participer à cette sécurisation peuvent aussi s'authentifier mutuellement, lors de leurs échanges en employant aussi des listes de codes comme décrit plus haut.
Tous les intervenants sont ainsi authentifiés mutuellement ce qui évite un échange avec un faux participant. Seul le porteur ne semble pas avoir d'indications fiables d'authentification ni du commerçant ni de la banque, il se fie aux indications fournies par le commerçant ou par un moniteur de caisse de celui-ci mais en fait le paiement ne peut être effectué que si la banque a authentifié son support ce qui équivaut pour le porteur à avoir authentifié sa banque si son compte est débité.
Pour augmenter la sécurisation du support objet de l'invention, le système peut permettre d'utiliser plusieurs codes au cours d'une même opération. Ces codes sont issus d'au moins une liste, un par un et dans l'ordre où ils sont inscrits sur le support comme décrit plus haut. S'il paraît peu probable de découvrir par le hasard quel est le bon code à un moment donné dans le déroulement de l'utilisation du support, il paraît impossible de découvrir, également par hasard, plusieurs codes successifs dans l'ordre où ils sont inscrits.
Par souci d'une utilisation simple du système il est préférable que chaque opération d'authentification soit réalisée automatiquement par chaque terminal de chaque participant.

Le dispositif selon l'invention se compose d'une part d'un support ayant les caractéristiques particulières décrites plus haut et d'autre part d'un système d'exploitation dans lequel intervient au moins un support tel que décrit, le système informatique de l'autorité en combinaison, lorsque c'est nécessaire, avec des lecteurs de supports et/ou des moyens de transmission et de traitement informatiques nécessaires à un échange.

Plusieurs variantes sont décrites ci-après dans lesquelles le support possède dans tous les cas la caractéristique de base qui est la présence d'au moins une liste de codes dont un seul à la fois est accessible comme il est décrit plus haut

sauf dans la première variante où cette caractéristique peut être modifiée.

Selon une première variante, au moins une liste de codes est complétée ou remplacée par au moins un algorithme capable de créer des mots, utilisables comme des codes, au fur et à mesure de la nécessité résultant de l'utilisation du support. Au moins un algorithme installé dans le système informatique de l'autorité crée les mêmes codes pour les comparer à ceux du support quand un échange avec ce support nécessite par exemple une authentification dudit support. De préférence ledit(lesdits) algorithme(s) n'est(ne sont) pas consultable(s) ou transformable(s) à partir du moment où il(s) est(sont) inscrit(s) dans le support.

Selon une autre variante, les données autres que les codes, concernant un échange, une opération en clair, codée ou cryptée peuvent être associées par le support ou par le système informatique avec lequel il communique, émetteur ou récepteur, à au moins un code d'au moins une liste de codes inscrite sur le support ce qui rend les données difficilement falsifiables et ce qui permet de coder un échange en clair. L'autorité étant la seule à connaître le ou les codes employés pour décoder cet échange, étant entendu que ces codes aussi sont de préférence différents à chaque échange. Pour une opération consistant en un paiement c'est l'assurance pour le porteur comme pour le commerçant que les données comme les conditions d'une commande, la référence d'un produit, le montant d'un paiement ne peuvent pas être modifiés au cours de l'échange.

Selon une autre variante le support n'est utilisable que pour des échanges de données et des télépaiements sécurisés depuis un ordinateur particulier, par exemple son ordinateur personnel ou un ordinateur spécifique d'une entreprise, pour échanger, avec un autre ordinateur. La lecture et l'exploitation dudit support nécessite un échange de données entre ledit support et l'ordinateur auquel il est lié induisant une reconnaissance mutuelle des deux éléments sans laquelle le support ne fournit pas les données qu'il possède et qui sont nécessaires à un échange avec un autre ordinateur afin de réaliser une opération particulière notamment un paiement. Le support est de préférence un disque qui peut être lu par un lecteur faisant partie intégrante de l'ordinateur ou un lecteur spécifique raccordé à cet ordinateur ce qui permet de donner au support la forme et l'apparence les plus diverses en plus de celles d'un disque. On limite ainsi le risque de vol du support qui peut être utilisé et conservé en un même lieu qui

peut n'être accessible qu'à l'utilisateur.
Le support n'est reconnu que par un seul matériel informatique auquel il est associé et ne peut être utilisé à partir d'un autre matériel même d'un type identique.

Selon une autre variante, la possibilité d'utiliser le support est subordonnée à l'entrée d'un code personnel propre à chaque porteur, secret, proposé au système du support grâce à un lecteur intégré dans le support ou par un lecteur classique ou par un ordinateur sans lecteur extérieur, à chaque utilisation, afin d'être reconnu par le support qui autorise le porteur à poursuivre sa procédure en vue d'un échange complet. Ledit code personnel varie dans le temps en tout ou partie suivant des modes que le porteur est seul à connaître et que le support reconnaît. Les variations sont choisies par le porteur avant la création du support parce qu'elles sont facilement mémorisables par le porteur en fonction, par exemple, de sa date de naissance, des jours ou des heures pairs ou impairs, des lettres d'un nom connu du porteur... Malgré ces variations, à un moment donné, un seul code personnel est valable et accepté par le support.

Selon une autre variante, au moins un code piégé peut bloquer l'utilisation du support. Certains porteurs inscrivent leur code personnel près de leur support, dans le cas d'une carte bancaire par exemple,pour le retrouver facilement en cas d'oubli. Malheureusement en cas de vol du support, il est probable que le voleur saura dans ce cas retrouver le code personnel pour utiliser délictueusement le support. Ledit code piégé est à inscrire de préférence sur le support ou à proximité, par exemple dans le portefeuille qui le contient. En cas d'utilisation d'un support volé avant que le porteur autorisé n'ait procédé aux formalités en vue de bloquer l'utilisation de ce support, si le voleur utilise ce code, comme un code personnel, ledit code est transmis à l'autorité qui interdit aussitôt toute opération en cours et à venir réalisée avec ce support et prévient le commerçant, s'il s'agit d'une opération de paiement auprès d'un commerçant que ce support est certainement volé; s'il s'agit d'une tentative d'utilisation dans une machine automatique comme un distributeur de billets, l'opération est refusée et le support peut être retenu bien que désormais inutilisable. S'il s'agit d'une erreur due à une manipulation du porteur authentique, ce dernier doit se rapprocher physiquement de l'autorité pour faire la preuve de son identité afin que l'utilisation de son support soit débloquée dans le système informatique de ladite autorité.

Selon une autre variante un dispositif de détection est associé au système pour s'assurer que chaque échange est transmis en totalité, en temps réel et sans interruption pour éviter qu'un échange puisse être soit en partie détourné, soit intercepté, modifié et réexpédier plus tard, soit intercepté, modifié et réexpédié en temps réel ou quasiment ce qui est plus difficile à réaliser. Ledit dispositif de détection, par exemple, émet au moins un signal qui peut être un signal d'horloge ou tout autre signal ayant la même fonction associé à tout ou partie des données d'un échange afin que ces données soient liées entre elles, identifiables et indissociables sauf en laissant une trace. Le système informatique de l'autorité détecte toute anomalie et peut réagir par exemple en demandant une confirmation ou en refusant l'authentification et le contenu de l'échange ou en refusant le paiement s'il s'agit d'une procédure de paiement.

Selon une variante complémentaire de la variante précédente, les caractéristiques du signal(des signaux) d'horloge ou de tout autre signal ayant la même fonction, varie(nt) dans un même échange et/ou sont différentes pour chaque échange. Le mode de ces variations est stocké dans une mémoire du support ainsi que dans la mémoire du système informatique de l'autorité qui contrôle la conformité des variations. Pour un observateur extérieur à la confidentialité desdites variations il est impossible de les prévoir ce qui rend impossible la production dudit signal, en temps réel, par un pirate qui tenterait de remplacer des données par de fausses données.
Toujours par souci de sécurisation, le mode desdites variations est de préférence inaccessible à la consultation sur le support même pour l'autorité, il se déroule au fur et à mesure de l'utilisation du support selon un plan préétabli.

Selon une autre variante, le support ne fournit, lorsqu'il est sollicité directement ou par un lecteur de supports, que des données permettant d'interroger l'autorité qui gère l'utilisation dudit support après quoi, dans le déroulement prévu de l'échange, l'autorité doit adresser vers ledit support des données particulières qui sont de préférence le premier code disponible d'une liste de codes dont on ne peut accéder qu'à un seul code à la fois dans les conditions décrites plus haut, inscrites dans une mémoire dudit support afin que ce dernier poursuive le déroulement de l'échange dès qu'il a reconnu ces données. Lorsque ces données sont reconnues comme venant de l'autorité, le support fournit des données permettant à l'autorité de l'authentifier. Cette variante dans l'utilisation des listes de codes évite en extrayant un code du support d'avoir la possibilité de

le détourner sur simple interrogation d'un lecteur de supports.
Si les données fournies au support, pour ouvrir un échange, par l'autorité ne correspondent pas à celles qu'il est prévu qu'il reçoive, ledit support ne continue pas l'échange. Mis à part les cas d'anomalies de fonctionnement dues à des pannes matériels, une telle configuration est certainement la conséquence d'une fausse autorité essayant de s'introduire parmi les intervenants authentiques. Une nouvelle tentative est de préférence possible mais le nombre de tentatives infructueuses autorisées pour une même opération ou pour des opérations successives est limité; après avoir épuisé ce nombre de tentatives, ledit support refuse l'échange et la communication du premier code prévu, reste fermé à tout échange ultérieur et le porteur doit se rapprocher physiquement de l'autorité pour trouver la cause de cette situation et s'assurer que le support fonctionne ou obtenir un autre support. De préférence ledit support est réutilisable au bout d'un laps de temps qui permet au porteur et à l'autorité de déterminer la nature du problème lors du dernier échange.
La tentative de piratage est ainsi vaicue:
Exemples: en supposant un support ayant une seule liste de codes accessibles comme décrit plus haut, pour la compréhension affectons à chaque code du début de cette liste un numéro de 1 à 3. Si le pirate essaie d'intercepter des codes pour accéder à un échange celà se passe ainsi:
1) le pirate, connecté au réseau ou à une ligne téléphonique interroge le support comme s'il était l'autorité, ne connaissant pas le code n°1 que doit fournir l'autorité pour poursuivre l'échange, le support ne poursuit pas l'échange, la tentative de piratage s'arrête là (de préférence cette tentative est signalée à l'autorité au prochain échange avec l'autorité par le support qui a enregistré l'incident).
2) - le pirate, connecté au réseau ou à une ligne téléphonique, interroge l'autorité comme s'il était un support autosisé; l'autorité adresse au pirate le code n°1 (en croyant l'adresser à un support authentique); avec ce code n°1 le pirate intercepte un début d'échange avec le support authentique (ce qui est déjà difficile), lui adresse le code n°1; le support reconnait le code et lui adresse en retour le code n°2 comme une authentification vis-à-vis de la vraie autorité; le pirate possède alors les codes n°1 et n°2 qu'il adresse alors à l'autorité comme venant d'un support autorisé et afin d'effectuer un échange complet, une transaction délictueuse...
- mais le code n°1 ayant déjà été échangé par l'autorité dans un échange précédent, n'est plus valable, l'autorité demandera au support (qui dans ce cas

est le pirate) de lui adresser le code n°3 que le pirate ne possède pas et l'échange ne sera ni certifié ni poursuivi.

- le pirate peut recommencer sa tentative pour obtenir le code suivant mais chaque fois il lui manquera le dernier code; de plus, après avoir obtenu le code n°1 de l'autorité, le pirate interromp l'échange (qu'il ne peut continuer ne possédant pas le code n°2) pour s'adresser au support au début de l'échange suivant avec l'autorité, concernant ce même support auquel le pirate essai de substituer un faux support, l'échange précédent ayant été interrompu, le système informatique de l'autorité va, de préférence, annuler le code n°1 concernant cet échange interrompu ainsi que le code suivant le n°2 (que lui propose le pirate) et demander le code n°3 que le pirate ne possède pas et il se retrouve dans les conditions du début alors que s'il ne s'agissait que d'un problème de transmission ou de mauvaise manipulation, le vrai support qui à déjà utilisé les codes n°1 et n°2 est prêt à utiliser le code n°3 et à poursuivre un échange sans interruption.

- au bout d'un certain nombre de tentatives de ce genre, de prérérence, le système informatique de l'autorité signale qu'il y a une tentative d'intrusion par tel support.

Selon une autre variante, à l'authentification du support s'ajoute, de préférence, l'identification du porteur c'est-à-dire son identification en tant que porteur autorisé d'un support déterminé.

Un premier moyen d'identification consiste en une photo d'identité intégrée au support de manière indissociable ce qui permet une identification pour un échange sur place par exemple lors d'un paiement chez un commerçant.

D'autres moyens permettent une identification du porteur sur place mais aussi à distance comme un lecteur spécialisé pour identifier le fond de l'oeuil, une empreinte digitale ou un code génétique à partir par exemple de la salive ou effectuant une reconnaissance vocale qui reconnait les paroles et identifie le porteur par comparaison à des voix mémorisées; ces moyens sont sûrs pour identifier un individu mais les données représentant cette identification peuvent être piratées afin d'être utilisées délictueusement c'est pourquoi, de préférence, cette identification s'ajoute à l'authentification du support pour former un ensemble sécurisé. Ledit lecteur spécialisé peut faire partie intégrante du support au moins pour la partie servant à l'identification.

Dans cette variante, à cette ensemble sécurisé, s'ajoute de préférence, au moins un dispositif secondaire associé au fonctionnement du support lors d'un échange ou de l'amorçage d'un échange. L'intervention dudit dispositif secondaire est

indispensable au fonctionnement du support sans quoi celui-ci n'échange pas quelle que soit la sollicitation extérieure. Chaque utilisation du support nécessite l'intervention dudit dispositif secondaire. Mis en relation avec le support, avec ou sans contact électrique, le dispositif secondaire n'est, de préférence, opérant que pendant un laps de temps prédéterminé pendant lequel le support peut soit être utilisé soit être amorcé pour être utilisé le temps nécessaire sans limitation; au delà de ce laps de temps qui peut être par exemple de quelques secondes ou de quelques minutes, ledit support nécessite à nouveau une intervention dudit dispositif secondaire pour échanger ou amorcer un échange.

Le vol dudit support ne peut permettre son utilisation qui doit être associée audit dispositif secondaire pour fonctionner.

La possession dudit dispositif secondaire peut être assimilée à une identification dans la mesure où ledit dispositif secondaire est attaché à son possesseur et peut rester secret tant dans son aspect que dans son lieu de fonctionnement; il peut être personnalisé et , de préférence, intégré dans un objet personnel du porteur tel que montre, bracelet, pendentif, ceinture, monture de lunettes ou même être implanté par exemple sous la peau pour les porteurs qui le désirent.

La source de courant électrique, rechargeable ou non, destinée au fonctionnement du/des système(s) permettant l'intervention dudit dispositif secondaire par rapport audit support, est disposée, suivant que le mode de fonctionnement est avec ou sans contact électrique, dans le dispositif secondaire et/ou dans le support; elle peut aussi n'être présente que dans le lecteur de supports et alimente alors l'ensemble lors de l'utilisation du lecteur.

Avantages du dispositif:

- dans un paiement ou un télépaiement c'est la banque ou la tierce partie à qui la banque a délégué son autorité qui décide de donner ou de refuser son accord pour une opération. Etant donné que c'est pratiquement sans risque, une banque peut garantir le bon fonctionnement du système de paiement et de télépaiement et prendre à sa charge tout risque de fraude ce qui est un atout essentiel pour augmenter le nombre de ses clients vis à vis de ce type de paiement.
- un support tel que décrit plus haut ne peut pas être reproduit puisque la liste de codes secrets n'est pas accessible et sans cette liste le support est inutilisable.
- sauf à choisir une forme nouvelle de supports, un lecteur spécifique n'est pas nécessaire; pour une carte de paiement, un lecteur classique de cartes suffit; ce n'est pas le lecteur qui assure la sécurisation, c'est le support et son lien avec l'autorité.

Revendications

1) Dispositif pour la sécurisation des échanges de données informatiques en vue notamment d'échanger des données confidentielles et/ou d'effectuer des paiements sur place ou des télépaiements utilisant des moyens informatiques caractérisé

- d'une part par un support comportant un système comportant des fonctions permettant,entre autres, de communiquer avec d'autres systèmes informatiques et ayant au mois une mémoire permettant de stocker des données sous forme de codes et/ou d'algorithmes, servant à l'authentification dudit support par l'autorité qui gère l'utilisation des supports tels que ledit support, et/ou à l'authentification mutuelle entre deux entités utilisant des moyens informatiques, ces codes et/ou ces algorithmes étant disposés de préférence dans au moins une liste rendue inaccessible à la consultation une fois qu'elle est inscrite dans ladite mémoire dudit support, sauf pour le premier code et/ou le premier algorithme de ladite liste qui peut être utilisé pour un échange, une fois et une fois seulement, après quoi il est écarté ou effacé ou rendu inaccessible et c'est le code et/ou l'algorithme suivant de ladite liste qui est alors le seul à pouvoir être consulté, utilisé comme code pour le même échange ou pour un autre échange, lesdits codes et/ou lesdits algorithmes se succédant de manière imprévisible pour un observateur extérieur à la confidentialité de leur composition et de leur disposition étant conçus et disposés de préférence de manière aléatoire par un logiciel et de préférence c'est le même logiciel qui crée au moins une seconde liste absolument identique à ladite liste inscrite dans le support, ladite seconde liste étant mise en mémoire dans le système informatique de ladite autorité ou d'une autre entité,
- d'autre part un système d'expoitation qui permet un échange de données en utilisant en combinaison au moins un support tel que ledit support et/ou ledit système informatique de ladite autorité et/ou d'une autre entité et/ou des moyens des moyens de transmission et de traitement informatiques nécessaires audit échange.

2) Dispositif selon la revendication 1, caractérisé en ce que au moins une liste de codes et/ou d'algorithmes du support objet de l'invention est complétée ou remplacée par un algorithme qui crée des codes et/ou des algorithmes utilisables comme ceux de ladite liste, au fur et à mesure de l'utilisation dudit support, au moins un algorithme installé dans le système informatique de ladite autorité créant les mêmes codes et/ou les mêmes algorithmes pour les comparer à ceux

dudit support permettant d'authentifier un support tel que ledit support lors d'un échange de données entre ledit support et ladite autorité et/ou une autre entité, et/ou permettant une authentification mutuelle entre ledit support et ladite autorité ou ladite entité.

3) Dispositif selon l'une quelconque des revendications précédentes, caractérisé par l'association par le système du support objet de l'invention d'au moins un code et/ou au moins un algorithme d'au moins une liste dudit support aux données échangées lors d'un échange.

4) Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que le support objet de l'invention n'est utilisable qu'avec un seul matériel informatique tel qu'un ordinateur ou un lecteur avec lequel il doit effectuer une reconnaissance mutuelle avant de pouvoir être exploitable.

5) Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que chaque utilisation du support est subordonnée à l'introduction dans le système dudit support et à son acceptation d'un code personnel propre audit support et au porteur authentique dudit support, ledit code personnel étant variable dans le temps, les variations étant secrètes sauf pour ledit porteur.

6) Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce qu'en cas d'utilisation d'un code particulier, ledit code déclenche le blocage de l'utilisation du support objet de l'invention dans le système informatique de ladite autorité, soit définitivement soit provisoirement.

7) Dispositif selon l'une quelconque des revendications précédentes, caractérisé par l'association au système d'exploitation d'un dispositif adjoint émettant au moins un signal qui peut être un signal d'horloge qui est associé à tout ou partie des données d'un échange, le système informatique de ladite autorité détectant, dans un échange grâce audit dispositif adjoint, toute anomalie dans l'échange des données pouvant indiquer une modification des données elles mêmes.

8) Dispositif selon la revendication 7 caractérisé en ce que les caractéristiques dudit signal(desdits signaux) varient dans un même échange et/ou pour chaque

échange, les modes de variations étant de préférence en mémoire et inaccessibles dans ledit support et dans ledit système informatique de ladite autorité.

9) Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit support ne fournit, lorsqu'il est sollicité directement ou par un lecteur de support, que les données permettant d'interroger ladite autorité qui gère l'utilisation dudit support, ladite autorité devant adresser, pour que l'échange se poursuive avec ledit support, des données particulières qui sont de préférence le premier code et/ou le premier algorithme d'au moins une desdites listes de codes et/ou d'algorithmes inscrite dans une mémoire dudit support, inaccessible, sauf à accéder au premier code et/ou au premier algorithme seulement comme décrit dans la revendication 1; après avoir reconnu lesdites données particulières, ledit support pouvant adresser à son tour des données à ladite autorité pour être authentifié et que l'échange puisse se poursuivre entre les deux entités mutuellement authentifiées, en cas d'échec de ladite authentification mutuelle une nouvelle tentative est possible, le nombre des tentatives étant de préférence limité.

10) Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que l'identification du porteur d'un support tel que selon l'invention se fait grâce à un dispositif secondaire indispensable à l'utilisation dudit support avant ou pendant un échange de données ou à l'amorçage d'un échange, avec ou sans contact électrique avec ledit support, ledit dispositif secondaire étant de préférence intégré dans un objet personnel dudit porteur et/ou en un lieu qui peut n'être connu que par ledit porteur même pendant l'utilisation dudit dispositif secondaire.